

**Privacy Impact Assessment (PIA)  
for  
Office of Inspector General (OIG)  
Office of Investigations Management System  
(OIMS)**



June 25, 2021

---

## PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

---

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC public-facing website,<sup>1</sup> which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

---

## SYSTEM OVERVIEW

---

The Office of Inspector General (OIG) Office of Investigations Management System (OIMS) assists the OIG in performing its investigative mission. The OIG's Office of Investigations (OI) carries out a nationwide program to prevent, detect, and investigate criminal, civil, or administrative wrongdoing and misconduct by FDIC employees and contractors, as well as to investigate complex and sophisticated crimes against FDIC insured financial institutions (FI), where perpetrators may be FI executives, insiders, customers, and other financial professionals. Crimes include bank fraud, money laundering, embezzlement, cybercrime, and currency manipulation. OI investigations are largely based upon referrals from the FDIC; law enforcement partners, including other OIGs; and the U.S. Department of Justice (DOJ), including U.S. Attorneys' Offices (USAO) and the Federal Bureau of Investigation (FBI). OI also assists in responding to OIG Hotline and Whistleblower allegations of suspected fraud, waste, abuse, and mismanagement, which may be received from FDIC employees, FDIC contractors or members of the public. OI maintains close and continuous working relationships with the DOJ; the FBI; other Offices of Inspector General; and federal, state, and local law enforcement agencies.

OIMS is comprised of three modules. The investigative tracking and support module of OIMS is maintained for the purpose of documenting, tracking, reviewing and reporting on all phases of OI investigative and litigation activities, and serves as a repository and source for information necessary to fulfill statutory reporting, access and disclosure requirements, including those pertaining to the Inspector General Act. The Hotline module is used to record and track information received by the OIG Hotline telephone or email service, which is operated by the OIG to provide a convenient way for FDIC employees, its contractors, and members of the public to report incidents of fraud, waste, abuse, and mismanagement within FDIC and its contractor operations, as well as crimes against FDIC insured FIs. The information could potentially be used for audit, administrative, and investigative purposes. The Whistleblower module provides a means for employees of the FDIC, financial institution employees and contractors to disclose violations of laws, rules, or regulations; gross mismanagement; gross waste of funds; or abuses of authority.

---

## PRIVACY RISK SUMMARY

---

In conducting this PIA of OIMS, we identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Transparency and Individual Participation
- Access and Amendment
- Data Minimization
- Purpose and Use Limitation

---

<sup>1</sup> [www.fdic.gov/privacy](http://www.fdic.gov/privacy)

### **Transparency and Individual Participation Risk:**

**Privacy Risk:** There is a risk that individuals may not be aware that their information is collected and maintained within OIMS, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

**Mitigation:** Given the nature of the OIG's investigative function and the need to maintain the confidentiality of associated investigative records and activities, this risk cannot be fully mitigated. This risk is mitigated to a large extent through the publication of this PIA, as well as the publication of FDIC SORN 30-64-0010, Investigative Files of the Office of Inspector General and FDIC SORN 30-64-0034, Office of Inspector General Inquiry Records. However, FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements regarding informing individuals of the authority, purpose, and routine uses of information collected with respect to the OIG investigative tracking and support module of OIMS, while information collected through the Hotline and Whistleblower modules of OIMS may also be exempt, as stipulated in FDIC SORN 30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

Access to certain information, such as the particulars concerning civil or criminal proceedings will be provided to an individual where a lawful requirement to provide such information exists. Further, most or all of the information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

### **Access and Amendment Risk:**

**Privacy Risk:** There is a risk that individuals may not have the opportunity to access their information or amend inaccurate information contained in OIMS.

**Mitigation:** This risk cannot be fully mitigated for records maintained within the OIG investigative tracking and support module of OIMS because providing individuals with the opportunity to access or amend certain information could impede or compromise an investigation. This risk is partially mitigated by the publication of this PIA, as well as FDIC SORN 30-64-0010, Investigative Files of the Office of Inspector General and FDIC SORN 30-64-0034, Office of Inspector General Inquiry Records. However, FDIC SORN 30-64-0010 reflects an exemption from Privacy Act requirements related to individual access and amendment with respect to the OIG investigative tracking and support module of OIMS, while information collected through the Hotline and Whistleblower modules of OIMS may also be exempt, as stipulated in FDIC SORN 30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

In the event of criminal or civil proceedings, an individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in those proceedings. The individual may also petition a court to direct FDIC to expunge or correct an error in an OIMS record.

### **Data Minimization Risk:**

**Privacy Risk:** There is a risk that the personally identifiable information collected within OIMS in the course of an investigation may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

**Mitigation:** This risk is mitigated by OIG investigative staff being appropriately trained. OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC agents' training is provided by the Federal Law Enforcement Training Center (FLETC) and the Inspector General Criminal Investigator Academy, which forms part of FLETC. Criminal investigator training for agents helps develop skills in interviewing subjects; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required annual training ensures that agents maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills. Additionally, OIG investigative staff limit the collection and maintenance of information to that necessary to thoroughly and fairly conduct investigations, while maintaining compliance with the OIG Records Disposition Program and FDIC Records Retention Schedules.

**Privacy Risk:** There is a potential risk that PII could be used in the test or lower environments beyond that which is necessary.

**Mitigation:** The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and to ensure all environments are secured appropriately based on the impact level of the information and the information system.

**Purpose and Use Limitation Risk:**

**Privacy Risk:** There is a limited, potential risk associated with use limitation for OIMS because sensitive information, including PII, stored in OIMS could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected.

**Mitigation:** This risk is mitigated by OIG staff being appropriately trained, including training specific to Federal law enforcement, and limiting OIG employee access to only that information needed for a business purpose, which is facilitated through the use of OIMS role-based access. This risk is further mitigated by OIG policies and procedures regarding the appropriate release of information.

---

## Section 1.0: Information System

---

### 1.1 What information about individuals, including personally identifiable information (PII) (e.g., name, Social Security number, date of birth, address, etc.) and non-PII, will be collected, used or maintained in the information system or project?

Information such as names, dates of birth, SSNs, Web URLs (personal), foreign activities and/or interests, and contact information is collected for individuals associated with investigations. For a member of the public's personally identifiable information to be included in OIMS, that individual must be associated with an OIG investigation. In addition, OIMS may include the personally identifiable information of FDIC employees, including that of OIG employees.

PII Element	Yes	No
Full Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth (DOB)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Place of Birth	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Social Security Number (SSN)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employment Status, History or Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mother's Maiden Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Home Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Number(s)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Identification Number (EIN)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Driver's License/State Identification Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Education Records	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Criminal Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Military Status and/or Records	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Investigation Report or Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Photographic Identifiers (e.g., image, x-ray, video)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other : Other potential investigative sources such as social media.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## 1.2 Who/what are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Members of the General Public	Members of the public may provide information via the OIMS Hotline and Whistleblower modules, or otherwise, regarding wrongdoing by individuals or banking institutions. The extent of the information provided greatly varies, but usually includes names and addresses.
FDIC Employees	FDIC employees, including FDIC OIG employees, may also submit information to the OIG, including through the OIMS Hotline and Whistleblower modules. The extent of the information provided varies, but may include, at a minimum, an individual's name, job position, and contact information. FDIC OIG personnel will also input PII for subjects and witnesses for ongoing criminal investigations.
Federal, State, Local agencies and Employees	Information is also often received from our Federal, State and local law enforcement partners. This information may include names, addresses, DOBs, SSNs, and financial account data and other identifiers.

## 1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

Yes, the system will be granted an ATO prior to use and will be periodically reviewed as part of the FDIC ongoing authorization process.

---

## Section 2.0: Transparency

---

*Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.*

### 2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

### 2.2 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

The investigative tracking and support module of OIMS operates under FDIC SORN 30-64-0010, Investigative Files of the Office of Inspector General, which covers investigative files, including memoranda, computer-generated background information, correspondence including payroll records, call records, email records, electronic case management, forensic, and tracking files, OIG Hotline related records, reports of investigations with related exhibits, statements, affidavits, records or other pertinent documents, reports from or to other law enforcement bodies, pertaining to violations or potential violations of criminal laws, fraud, waste, and abuse with respect to administration of FDIC programs and operations, and violations of employee and contractor Standards of Conduct as set forth in section 12(f) of the Federal Deposit Insurance Act (12 U.S.C. 1822(f)), 12 CFR parts 336, 366, and 5 CFR parts 2634, 2635, and 3201. Records in this system may contain personally identifiable information provided or obtained in connection with an investigation.

The Hotline and Whistleblower modules of OIMS operate under FDIC SORN 30-64-0034, Office of Inspector General Inquiry Records, which covers individuals, including, but not limited to, members of the public, the media, contractors and subcontractors, Congressional sources, and employees of the FDIC or of other governmental agencies, who communicate with the OIG through written or electronic correspondence or telephonically, including the OIG Hotline. The system also includes

individuals who receive correspondence from the OIG and those who are the subject of correspondence to or from the OIG. As stipulated in FDIC SORN 30-64-0034, records transferred from the Hotline and Whistleblower modules of OIMS to the investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010 referenced above.

**2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.**

While OIMS is a new system, the SORNs will not require amendment or revision. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

**2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.**

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1 'FDIC Forms Management Program.'

Most PII information input to the investigative tracking and support module of OIMS is obtained during the course of a criminal investigation. Providing a Privacy Act notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with the OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

The public facing Hotline and Whistleblower modules provide individuals with the ability to input various types of information, including PII, the extent of which may vary greatly. The Hotline and Whistleblower modules contain Privacy Act Statements prior to the input and submission of any information. Callers to the OIG Hotline/Whistleblower telephone number are directed via recorded message to access the respective OIMS modules to provide information or alternatively to provide the information via either U.S. Mail or email.

**2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.**

The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records Clearance Officer, and the Privacy Program (Privacy@fdic.gov). The Protecting Privacy subpage discusses general practices related to the Privacy Act and PII. See <https://www.fdic.gov/about/privacy/protecting.html>.

FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements related to notification and access with respect to the OIG investigative tracking and support module of OIMS.

Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

## **Privacy Risk Analysis: Related to Transparency**

**Privacy Risk:** There is a risk that individuals may not be aware that their information is collected and maintained within OIMS.

**Mitigation:** Given the nature of the OIG's investigative function and the need to maintain the confidentiality of associated investigative records and activities, this risk cannot be fully mitigated. However, the risk is mitigated to a large extent through the publication of this PIA and the SORNs referenced in Section 2.2. However, FDIC SORN 30-64-0010, reflects an exemption from the Privacy Act requirements related to notification and access with respect to the OIG investigative tracking and support module of OIMS, while information collected through the Hotline and Whistleblower modules of OIMS may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

Access to certain information, such as the particulars concerning civil or criminal proceedings will be provided to an individual where a lawful requirement to provide such information exists. Further, most or all of the information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

---

## **Section 3.0: Access and Amendment**

---

*Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.*

### **3.1 What are the procedures that allow individuals to access their information?**

The OIG investigative tracking and support module of OIMS does not have procedures for individual access. The PII maintained within the module is contained in a Privacy Act System of Record that has been exempted from the Privacy Act individual access requirement. Providing access to the records contained in the investigative tracking and support module of OIMS could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of FDIC or another agency. Additionally, access to the records could permit the individual who is the subject of an investigation to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. In addition, permitting access to such information could disclose security-sensitive information that could be detrimental to the FDIC.

Access procedures for the Hotline and Whistleblower modules of OIMS are detailed in FDIC SORN 30-64-0034. However, as noted in that SORN, records transferred from those modules to the OIG investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010, which include an exemption from the Privacy Act individual access requirement.

Access to certain information, such as the particulars concerning civil or criminal proceedings will be provided to an individual where a lawful requirement to provide such information exists. In addition, most or all of the information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

### 3.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The investigative tracking and support module of OIMS does not have procedures to allow individuals to correct inaccurate or erroneous information. The PII maintained by the system is contained in a Privacy Act System of Record that has been exempted from the Privacy Act redress requirement.

During the course of investigations, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to the FDIC.

Procedures for correcting records associated with the Hotline and Whistleblower modules of OIMS are detailed in FDIC SORN 30-64-0034. However, as noted in that SORN, records transferred from those modules to the OIG investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010, which include an exemption to the access and amendment requirements of the Privacy Act.

An individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in relevant criminal or civil proceedings. The individual may also petition a court to direct FDIC to expunge or correct an error in an OIMS record.

### 3.3 How does the information system or project notify individuals about the procedures for correcting their information?

As indicated in FDIC SORN 30-64-0010, the PII maintained in the investigative tracking and support module of OIMS is contained in a Privacy Act System that has been exempted from the access and amendment requirements of the Privacy Act.

Procedures for correcting records associated with the Hotline and Whistleblower modules of OIMS are detailed in FDIC SORN 30-64-0034. However, as noted in that SORN, records transferred from those modules to the OIG investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010, which include an exemption from the Privacy Act access and amendment requirements.

## Privacy Risk Analysis: Related to Access and Amendment

**Privacy Risk:** There is a risk that individuals may not have the opportunity to access their information or amend inaccurate information contained in OIMS.

**Mitigation:** This risk cannot be fully mitigated for records maintained within the OIG investigative tracking and support module of OIMS because providing individuals with the opportunity to access or amend certain information could impede or compromise an investigation. This risk is partially mitigated by the publication of this PIA, as well as FDIC SORN 30-64-0010, Investigative Files of the Office of Inspector General and FDIC SORN 30-64-0034, Office of Inspector General Inquiry Records. However, FDIC SORN 30-64-0010 reflects an exemption from Privacy Act requirements related to individual access and amendment with respect to the OIG investigative tracking and support module of OIMS, while information collected through the Hotline and Whistleblower modules of OIMS may also be exempt, as stipulated in FDIC SORN 30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

In the event of criminal or civil proceedings, an individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in those proceedings. The individual may also petition a court to direct FDIC to expunge or correct an error in an OIMS record.

---

## Section 4.0: Accountability

---

*Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.*

### **4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.**

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy and guidance. This includes the Privacy Act of 1974<sup>2</sup>, as amended; Section 208 of the E-Government Act of 2002<sup>3</sup>, Section 522 of the 2005 Consolidated Appropriations Act,<sup>4</sup> Federal Information Security Modernization Act of 2014,<sup>5</sup> Office of Management and Budget (OMB) privacy policies, and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Section Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional information security managers located within the agency's divisions and offices.

### **4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.**

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

### **4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?**

Privacy risks posed by OIMS are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, <https://www.fdic.gov/about/privacy/index.html>.

---

<sup>2</sup> The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

<sup>3</sup> Section 208 of the E-Government Act of 2002, Public Law No. 107-347, 44 U.S.C. Ch. 36.

<sup>4</sup> Consolidated Appropriations Act, 2005, Public Law No. 108-447, Division H, Title V, Section 522.

<sup>5</sup> The Federal Information Security Management Act of 2014, Public Law No: 113-283, 44 U.S.C. § 3554.

**4.4 What roles, responsibilities and access will a contractor have with the design and maintenance of the information system or project?**

Contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

**4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?**

Yes, Confidentiality Agreements/Non-Disclosure Agreements have been completed and signed for contractors who work on OIMS. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

**4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?**

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program is currently in the process of implementing a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

**4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.**

OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC agents' training is provided by the FLETC and the Inspector General Criminal Investigator Academy, which forms part of FLETC. Criminal investigator training for agents helps develop skills in interviewing subjects; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required annual training ensures that agents maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills.

The FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

**4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.**

The FDIC Privacy Section develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; and Information Security Manager's Monthly meetings.

**4.9 Explain how this information system or project protects privacy by automating privacy controls?**

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls if possible.

As part of the internal technical controls within OIMS, case files are restricted to those persons with a need to know. Each record has an audit trail to track the modification and who made the changes (by person and date/time stamp).

Additionally, FDIC has implemented technologies to track and manage PII inventory, as well as to track, respond, remediate and report on breaches. Breaches are handled in accord with FDIC's Breach Response Plan.

**4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?**

Disclosures are not made directly from OIMS. Disclosures of information held under FDIC SORN 30-64-0010 and FDIC SORN 30-64-0034 are made pursuant to the established routine uses as documented in the SORNs. FDIC SORN 30-64-0010 provides an exemption from making accounting of disclosures available to individuals. Additionally, as stipulated in FDIC SORN 30-64-0034, records transferred from the Hotline and Whistleblower modules to the OIG investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010.

**4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?**

Disclosures are not made directly from OIMS. Disclosures of information held under FDIC SORN 30-64-0010 and FDIC SORN 30-64-0034 are made pursuant to established routine uses as documented in the SORNs. FDIC SORN 30-64-0010 provides an exemption from making accounting of disclosures available to individuals. Additionally, as stipulated in FDIC SORN 30-64-0034, records transferred from the Hotline and Whistleblower modules of OIMS to the OIG investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010.

**4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?**

Disclosures are not made directly from OIMS. Disclosures of information held under FDIC SORN 30-64-0010 and FDIC SORN 30-64-0034 are made pursuant to established routine uses as documented in the SORNs. FDIC SORN 30-64-0010 provides an exemption from making accounting of disclosures available to individuals. Additionally, as stipulated in FDIC SORN 30-64-0034, records transferred from the Hotline and Whistleblower modules of OIMS to the OIG investigative tracking and support module of OIMS are subject to the exemptions claimed under FDIC SORN 30-64-0010.

## **Privacy Risk Analysis: Related to Accountability**

**Privacy Risk:** There are no identifiable risks associated with accountability for OIMS.

**Mitigation:** No mitigation actions are recommended.

---

## Section 5.0: Authority

---

*Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.*

### 5.1 **Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).**

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Circular 1360.20, FDIC Privacy Program, mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws:

- The IG Act of 1978, as amended, provides the FDIC OIG with oversight responsibility of the programs and operations of the FDIC.
- 12 USC 1819 states that FDIC can make examinations of and to require information and reports from depository institutions.
- 12 USC 1820 discusses examinations and the authority of FDIC to make and keep copies of information for FDIC's use.
- 12 USC 1821 deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving banks. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 USC 1822 deals with FDIC as a Receiver of failed banks.
- 12 CFR 330 clarifies the rules and define the terms necessary to afford deposit insurance coverage under the Act and provide rules for the recognition of deposit ownership in various circumstances.
- 12 CFR 366 deals with FDIC contractors.
- 5 CFR 720 deals with Affirmative Action.
- 5 U.S. Code § 7201 deals with antidiscrimination policy; minority recruitment program.

## Privacy Risk Analysis: Related to Authority

**Privacy Risk:** There are no identifiable risks associated with authority for OIMS.

**Mitigation:** No mitigation actions are recommended.

---

## Section 6.0: Minimization

---

*Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.*

### 6.1 **How does the information system or project ensure that it has identified the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?**

FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirement regarding the maintenance of records that are relevant and necessary with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS. However, the PII elements contained within OIMS are relevant and necessary to support the OIG's investigative functions and activities. Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

**6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?**

FDIC SORN 30-64-0010 reflects an exemption from Privacy Act requirements related to notification and the maintenance of records that are relevant and necessary with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

The PII elements contained within OIMS are relevant and necessary to support the OIG's investigative functions and activities. OIG investigators undergo extensive training, including Federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries, and the OIG has policies and procedures in place addressing individuals' rights and obligations that vary depending on the type of investigation and on whether the individual is a Federal employee.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

**6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?**

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

**6.4 What are the retention periods of data in this information system? or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.**

OIMS records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual, National Archives and Records Administration (NARA)-approved record retention schedule, and the OIG's policies and procedures related to the OIG Records Disposition Program, as follows:

- Records having national media attention, involving a Congressional investigation, and/or that have been deemed to have historical value may be held permanently.
- Files containing information or allegations which are of an investigative nature, but do not relate to a specific investigation, are deleted/destroyed after five years. These records include OIG Hotline files, anonymous or vague allegations not warranting an investigation, matters referred to constituents or other agencies for handling, and support files providing general information which may prove useful in Inspector General investigations.
- Files developed during investigations are deleted/destroyed ten years after the cases are closed. These records include cases of known or alleged fraud and abuse, and irregularities and violations of laws and regulations, including hotline cases related to specific investigations.

**6.5 What are the policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?**

PII in this system is not used for testing, training, or research. Use of sensitive data outside the production environment requires the management approval via a waiver. Any production data, including PII, may not be used outside of the production environment unless a waiver has been approved by management, and appropriate controls have been put in place.

## **Privacy Risk Analysis: Related to Minimization**

**Privacy Risk:** There is a risk that the personally identifiable information collected within OIMS in the course of an investigation may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

**Mitigation:** This risk is mitigated by OIG investigative staff being appropriately trained. OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC agents' training is provided by the FLETC and the IG Criminal Investigator Academy, which forms part of FLETC. Criminal investigator training for agents helps develop skills in interviewing subjects; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required annual training ensures that agents maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills. Additionally, OIG investigative staff limit the collection and maintenance of information to that necessary to thoroughly and fairly conduct investigations, while maintaining compliance with the OIG Records Disposition Program and FDIC Records Retention Schedules.

**Privacy Risk:** There is a potential risk that PII could be used in the test or lower environments beyond that which is necessary.

**Mitigation:** The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and to ensure all environments are secured appropriately based on the impact level of the information and the information system.

---

## **Section 7.0: Data Quality and Integrity**

---

*Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual*

**7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.**

The OIG's Office of Investigations has an editing and review process for all OIG Reports of Investigations. Agents are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats where appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Methods may include reference to commercial databases to: obtain background information; verify addresses, identities, and contact information; trace proceeds from illegal activities; identify possible witnesses; and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. The OIG verifies records by checking every incoming complaint to ensure that the OIG has not received the same complaint previously. If so, the OIG cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue. The OIG also updates OIMS with timely information on referrals, administrative actions,

prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirement related to the accuracy, relevance, timeliness, and completeness of records maintained with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

Additionally, the FDIC reviews privacy artifacts for adequate measures to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

**7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?**

FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirement related to the collection of PII directly from individuals with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

OIG investigators collect and analyze evidence through a number of techniques, including interviews of complainants, witnesses, victims, and subjects; reviews of records (e.g., personnel files, contract or grant files, financial records, etc.); collection of forensic evidence; surveillance and consensual monitoring; and use of computer technology (e.g., link analysis, databases, spreadsheets, cyber forensics, data mining, etc.). The decision-making process with respect to what information is required for a specific investigation and how that information should be obtained, varies considerably depending on the type of investigation underway.

Additionally, OIG investigators undergo extensive training, including Federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries, and the OIG has policies and procedures in place addressing individuals' rights and obligations that vary depending on the type of investigation and on whether the individual is a Federal employee.

**7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.**

The FDIC reviews privacy artifacts to ensure adequate measures to check for and correct any inaccurate or outdated PII in its holdings.

**7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.**

The OIG's Office of Investigations has an editing and review process for all OIG Reports of Investigations. Agents are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats where appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Methods may include reference to commercial databases to: obtain background information; verify addresses, identities, and contact information; trace proceeds from illegal activities; identify possible witnesses; and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. The OIG verifies records by checking every incoming complaint to ensure that the OIG has not received the same complaint previously. If so, the OIG cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue.

The OIG also updates OIMS with timely information on referrals, administrative actions, prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

However, FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirement related to the accuracy, relevance, timeliness, and completeness of records maintained with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

**7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.**

OIMS has technical security measures and controls in place to prevent the misuse of data. Such security measures and controls consist of: user identification and authentication, network/database permissions, automatic session lockout after a period of inactivity, automatic account lockout after a specified number of failed logon attempts, strong password requirements, and the deployment of firewalls that protect network connections and prevent unauthorized access. OIMS also uses data encryption when data is transferred to and from the applications database and user workstations. System user access to cases is controlled using case access lists that are based on a person's need to know. Further, FDIC employees must complete FDIC's Corporate Information Security and Privacy Awareness Training on an annual basis.

Through its PTA adjudication process, the FDIC Privacy Program utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer configures administrative and technical controls for the system or project based on the FIPS 199 determination.

**7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?**

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988, and consequently does not have a need to establish a Data Integrity Board.

## **Privacy Risk Analysis: Related to Data Quality and Integrity**

**Privacy Risk:** There are no identifiable risks associated with data quality and integrity for OIMS.

**Mitigation:** No mitigation actions are recommended.

---

## **Section 8.0: Individual Participation**

---

*Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.*

**8.1 Explain how the information system or project provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.**

Most PII information input to the investigative tracking and support module of OIMS is obtained during the course of a criminal investigation. Providing notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with the OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

Depending on the nature of the investigation, OIG investigators may ask persons if they wish to consent to particular uses of the information they provide – for example, if an individual requests confidentiality they will be advised of the extent to which confidentiality can be provided under applicable laws and regulations.

With respect to the Hotline and Whistleblower modules, the OIG provides information about the Privacy Act to complainants on the online forms, which provide individuals with an understanding of the consequences of approving or declining the authorization of the collection, use, dissemination, and retention of PII. If a Hotline or Whistleblower complainant wishes to remain anonymous, the complaint can be submitted without the inclusion of any PII.

Additionally, this PIA and the SORNs referenced in 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

It should be noted, however, that FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

## **8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.**

Most PII information input to the investigative tracking and support module of OIMS is obtained during the course of a criminal investigation. Providing notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

Depending on the nature of the investigation, OIG investigators may ask persons if they wish to consent to particular uses of the information they provide – for example, if an individual requests confidentiality they will be advised of the extent to which confidentiality can be provided under applicable laws and regulations.

With respect to the Hotline and Whistleblower modules, the OIG provides information about the Privacy Act to complainants on the online forms, which provide individuals with an understanding of the consequences of approving or declining the authorization of the collection, use, dissemination, and retention of PII. If a Hotline or Whistleblower complainant wishes to remain anonymous, the complaint can be submitted without the inclusion of any PII.

Additionally, this PIA and the SORNs referenced in 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

It should be noted, however, that FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

**8.3 Explain how the information system or project obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.**

As appropriate, the FDIC Privacy Program will update and publish the relevant Privacy Act SORN(s), as well as the relevant PIA, to reflect any new uses or disclosures.

It should be noted, however, that FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

**8.4 Explain how the information system or project ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.**

OIMS only uses PII for the purposes listed in Section 9.1 of this PIA. This PIA and FDIC SORNs 30-64-0010 and 30-64-0034 serve as notice for all uses of the PII.

However, it should be noted that FDIC SORN 30-64-0010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the OIG investigative tracking and support module of OIMS. Additionally, information collected through the Hotline and Whistleblower modules may also be exempt, as stipulated in FDIC SORN-30-64-0034, if the records are transferred to the OIG investigative tracking and support module of OIMS.

**8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?**

The FDIC Privacy Program website, <https://www.fdic.gov/about/privacy/index.html>, instructs viewers to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

## **Privacy Risk Analysis: Related to Individual Participation**

**Privacy Risk:** There is a risk that individuals will not know how their data is being used or shared, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

**Mitigation:** Given the nature of the OIG's investigative function and the need to maintain the confidentiality of associated investigative records and activities, this risk cannot be fully mitigated. However, the risk is mitigated to a large extent through the publication of this PIA, as well as the publication of the SORNs referenced in Section 2.2. However, FDIC SORN 30-64-0010, reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the OIG investigative tracking and support module of OIMS, while information collected through the Hotline and Whistleblower modules of OIMS may also be exempt if the records are transferred to the OIG investigative tracking and support module of OIMS.

Access to certain information, such as the particulars concerning civil or criminal proceedings will be provided to an individual where a lawful requirement to provide such information exists. Further, most or all of the information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

---

## Section 9.0: Purpose and Use Limitation

---

*Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.*

**9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.**

The OIG collects information in order to meet its responsibilities under the Inspector General Act to conduct investigations relating to FDIC programs and operations. The OIG collects information only where the OIG has specific legal authority to do so and the information is required to meet the OIG's responsibilities, including those expressly established under the Inspector General Act. Commercial data is sometimes collected as background information; to verify addresses, identities, and business data. Investigative data is only shared within and among other law enforcement agencies as needed to further the investigation.

**9.2 Describe how the information system or project uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.**

Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 'Protecting Sensitive Information' with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Access to all investigative information is based on a business need to know. Users of OIMS include authorized OIG Office of Investigations staff and authorized OIG Executive Management and Counsel to the Inspector General. Information Technology Staff of the OIG's Office of Management have access to OIMS for system support purposes. A limited number of FDIC Division of Information Technology Local Area Network Management system administrators also have access to the OIMS database for the purpose of supporting hardware and network services.

**9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.**

Access to all investigative information is based on a business need to know. Access to OIMS requires individuals to be active users of the FDIC network. The FDIC's Access Request and Certification System (ARCS) is used to facilitate the tracking and management of FDIC employees that are OIMS users. ARCS requests must be submitted by users and approved by managers in order to gain access to OIMS. User access is further controlled and restricted according specific user and administrative roles that have been defined and established within OIMS.

**9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.**

- ☒ No  
☐ Yes

Explain.

**9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?**

No, OIMS does not aggregate or consolidate data in order to make determinations or derive new data about individuals.

**9.6 Does the information system or project share personally identifiable information (PII) externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used. Please explain.**

Information is shared externally pursuant to the routine uses described in the SORNs referenced in Section 2.2.

Additionally, through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1031.1 'Administration of the Privacy Act', and FDIC Circular 1360.17 'Information Technology Security Guidance for FDIC Procurements/Third Party Products'. The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9

**9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.**

Access to all investigative information is based on a business need to know. Access to OIMS requires individuals to be active users of the FDIC network. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established within OIMS.

OIG investigators undergo extensive training, including Federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries. The OIG has policies and procedures in place addressing the rights and obligations of individuals that vary depending on the type of investigation and on whether the individual is a Federal employee.

Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

**9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.**

OIG investigators undergo extensive training, including Federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries. The OIG has policies and procedures in place addressing the release of information and the rights and obligations of individuals that vary depending on the type of investigation and on whether the individual is a Federal employee.

Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Further, the FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

## **Privacy Risk Analysis: Related to Purpose and Use Limitation**

**Privacy Risk:** There is a limited, potential risk associated with purpose and use limitation for OIMS because sensitive information, including PII, stored in OIMS could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected.

**Mitigation:** This risk is mitigated by OIG staff being appropriately trained and limiting OIG employee access to only that information needed for a business purpose, which is facilitated through the use of OIMS role-based access. This risk is further mitigated by OIG policies and procedures that address the appropriate release of information.

---

## **Section 10.0: Security**

---

*Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.*

### **10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing personally identifiable information (PII).**

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC conducts an evaluation of information in the systems to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

### **10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?**

The FDIC Privacy Program updates the Chief Information Security Officer (CISO) on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

### **10.3 Has a Privacy Incident Response Plan been developed and implemented?**

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

### **10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?**

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

## **Privacy Risk Analysis: Related to Security**

**Privacy Risk:** There are no identifiable risks associated with security for OIMS.

**Mitigation:** No mitigation actions are recommended.